Fermilab

July 11, 2001

To: Metasys Working Group
From: Keith Chadwick / Data Communications Department
Subject: Metasys Network Scenarios

In an isolated island vs. Fermilab network scenario, what are the Pros and Cons of each approach?

The significant advantage of an isolated Metasys Ethernet network is that the Metasys network security occurs at the physical layer of the network **as long as no-one interconnects the two networks**.

There are significant disadvantages to the approach of a fully isolated Metasys network:

- There are many locations on site where a PC connected to the general purpose network would be adjacent to a PC connected to the isolated Metasys network. While PC costs have fallen rapidly, placing two PC's where it would be possible to use one PC for both functions would be a less than optimal solution.

- There would be an ongoing effort required to assure that the isolated Metasys network remains isolated. In the case of the aforementioned office with two PC's, all that would be required to cross connect the two networks, would be an Ethernet crossover patch cord (available at CompUSA or Best Buy), and a mistake by the office occupant.

- Significant amounts of additional network infrastructure would be required to fully implement an isolated Metasys network across the entire Fermilab site.

- A fully isolated Metasys network would preclude the use of tools such as M-Web from the site wide general purpose network, or other tools which would allow building managers the ability to connect to Fermilab via the Internet and monitor their buildings.

The biggest concerns in the case of an integrated Metasys Ethernet network would be related to the security of Metasys. As it stands today, the Metasys system is very insecure. Engineering efforts are underway within Johnson Controls Incorporated (JCI) to address security and related issues in their product line, but for the next few years, we

(Fermilab) must deal with the products available today and their current (lack of) security. Addressing these security concerns appears to be well within the capabilities of products already on the market (Cisco PIX firewall and Cisco VPN concentrators).

An integrated Metasys Ethernet network would allow use of tools such as M-Web, and could offer significant advantages for both Metasys supporters and building managers. Building managers could utilize the VPN access from home via the Internet to proactively monitor their systems, and take (authorized) actions to address any exceptions without driving into Fermilab during off hours.

If the CD/Data Communications Department were to setup the IP infrastructure for Metasys, what would be the proposal? How can this part of the network be secured? (Firewall?)

Securing the Metasys Network:

Ken Fidler's analysis of M-Web security demonstrates that the basic Metasys network protocols are insecure, we must consider to what level and how to secure the Metasys network. While Johnson Controls, Inc. (JCI) has repeatedly stated that "to-date, Metasys has not been hacked", Fermilab would be foolish to base the network security on that statement, given the availability of network sniffers. Furthermore, since the M-Web software bypasses the security controls in the Metasys OWS server, any random internet user could install the M-Web software on their home PC and point it at a Fermilab Metasys OWS server, and start changing set points on Fermilab equipment. These security holes must be addressed if Fermilab is going to connect the Metasys network to the site wide general purpose network.

For the past several months, the Data Communications department has operated a low end Cisco VPN concentrator and Cisco PIX firewall to isolate our department desktops and certain file servers from the general Fermilab networks as well as the general Internet. These devices have served the intended purpose well, isolating our Departments systems from the nearly constant scanning originating from the general Internet, as well as the more focussed scanning which has originated in-house (ISS scanning by Randy Rietz).

The PIX firewall is configured with a "default deny" for all connections which originate outside the DCD network, and a "default allow" for all connections which originate within the DCD network. The PIX firewall can be through of as a "network diode" which only allows network traffic to originate from within the protected portion of the network. The VPN concentrator allows a user from outside the DCD network (such as at home) to authenticate into the firewall protected network and access resources as though they were within the DCD network (thus bypassing the "network diode").

The experience that Data Communications Department has gained in the operation of these devices has led to DCD Design Note 173.1 “Facility Perimeter-Protected Network” which proposes the acquisition of a high end Cisco VPN concentrator and Cisco PIX firewall to isolate significant portions of the Fermilab network from the general Internet. The Data Communications Department is actively procuring the appropriate Cisco VPN concentrator and Cisco PIX firewall hardware to begin implementation of the perimeter protected network, and expects to have them on site no later that September 30, 2001.

Protection of the Metasys Ethernet network could take one of two forms:

1. Utilize the PIX and VPN devices which are part of the Facility Perimeter Protected Network (see DCD Design Note 173.1), or
2. Acquire PIX and VPN devices (typically lower performance), which would be dedicated to the protection of the Metasys network.

Selection of option 1 would still leave the Metasys network at risk for the inadvertent or deliberate actions of Fermilab employees and users. Selection of option 2 would address that concern, albeit at a slightly higher cost.

Migration of the Metasys Network from Arcnet to Ethernet:

To convert the Metasys network from the existing Arcnet infrastructure to Ethernet a multi step plan would be recommended to assure continued operation of the Metasys network:

1. Convert the core of the existing Metasys network from Arcnet to Ethernet, add appropriate network based security, and interconnect the Metasys Ethernet to the remainder of the Fermilab network.
2. Upgrade the Metasys Network Control Modules in Wilson Hall.
3. Upgrade the outlying Metasys Modhubs and remaining NCMs.
4. Extend the Metasys Ethernet to new buildings and locations.

Note that work on steps 2, 3 and 4 could overlap once the core of the Metasys network has been migrated to Ethernet, subject to personnel resources and availability.

Conversion of the Core Metasys Network:

1. Install Ethernet hubs with Fiber uplinks adjacent to the three Metasys Arcnet modhubs located in the Wilson Hall basement, Central Utility Building and the Feynman Computing Center.

2. Install Ethernet adapter boards in the three Metasys modhubs and interconnect the modhubs to the adjacent Ethernet hubs.

3. Install an appropriate Ethernet switch (or partition an existing switch that has sufficient resources) in Wilson Hall Fiber Central (WH8.4) for the core of the Metasys network. Install a Cisco VPN concentrator and (optionally) a Cisco PIX firewall between the Metasys network and the Wilson Hall core 6509 switch/router.

4. Install air blown fiber in existing tubecable between:

   4.1. WH8.4 and CUB.

   4.2. WH8.4 and the Wilson Hall modhub in the Wilson Hall Basement

5. Transition the Metasys links between CUB to Wilson Hall and Wilson Hall to FCC from the Arcnet network to the new Ethernet links and switch in WH8.4.

6. Relocate the M-Web server and the Metasys Ethernet to Arcnet gateway machines into the secured Metasys network.

Conversion of the Metasys Network Control Modules (NCMs) in Wilson Hall:

1. For those NCMs that can be upgraded in place, order the new Ethernet interface. While waiting for the interface delivery, submit appropriate network installation requests for optical fiber.

2. For those NCMs that cannot be upgraded in place, order new NCM with Ethernet interfaces. While waiting for the "forklift" upgrades, submit appropriate network installation requests for optical fiber.

3. For most floors in Wilson Hall, the implementation of a network installation request will involve the installation of a short (less than 50') optical fiber jumper from the closest network "point of presence". For locations on the 4th, 15th, 16th and some locations on the ground floor, additional single cell tubecable and fiber would be required.

Conversion of the outlying Metasys Modhubs and NCMs:

As with the conversion of the Metasys modhubs and NCMs in Wilson Hall, once the core of the Metasys network is converted from Arcnet to Ethernet, the remaining Modhubs and NCMs in areas such as CUB, CDF, FCC can be converted on an incremental and ongoing basis. Existing available fiber and Category 5 Ethernet cabling can be allocated for the conversion of the Metasys network, and additional fiber or Category 5 Ethernet cabling can be installed where necessary.

Expansion of the Metasys Ethernet into new buildings and locations:

To expand the Metasys Ethernet network into new buildings and locations, there are three options:

1. Allocation of existing network infrastructure to the Metasys network.
2. Install new or additional network infrastructure for the Metasys network.
3. Install necessary equipment to utilize VLAN trunking on the existing network link to the appropriate network concentration point (WH, FCC, EAD, Site 38, Village, etc.).

The selection of option 1, 2 or 3 can be made on an economic basis. In some cases (example: the run from FCC to Site 38/39), it may be advantageous to install additional network infrastructure, rather than utilizing VLAN trunking in order to position the network to best support future demands for network services. Of course, in areas where network infrastructure does not exist we will have no alternative than to install new network infrastructure.